Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I

Margo Utomo, Ahmad Holil Noor Ali, Irsal Affandi
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111
E-mail: holil@its-sby.edu

Abstrak **– Perkembangan teknologi informasi yang pesat saat ini turut berimbas kepada penggunaan teknologi informasi di lingkungan pemerintahan. KPPN Surabaya I sebagai instansi vertikal dari Direktorat Jenderal Perbendaharaan juga menerapkan teknologi informasi dalam untuk mendukung kegiatan pelayanan terhadap satuan kerja yang berada di lingkup bayarnya. Sayangnya masalah keamanan informasi yang merupakan bagian penting dari teknologi informasi sering kali kurang mendapatkan perhatian. Tidak dapat dipungkiri bahwa munculnya ancaman ataupun kelemahan dalam teknologi informasi dapat menggangu jalannya kegiatan pelayanan yang menggunakan teknologi informasi. Oleh karena itu diperlukan pengelolaan teknologi informasi berbasis risiko yang dituangkan dalam tata kelola untuk mengelola ancaman ataupun kelemahan yang muncul. ISO/IEC 27001:2005 merupakan framework sistem manajemen keamanan informasi yang dapat dijadikan dasar dalam pengelolaan keamanan informasi. Tata kelola keamanan informasi yang dibuat ini menitikberatkan pada kontrol akses yang merupakan salah satu kotrol keamanan dari ISO/IEC 27001:2005**

Kata Kunci**— teknologi informasi, keamanan informasi, tata kelola, kontrol akses, *ISO/IEC 27001:2005*.**

I. PENDAHULUAN

KEAMANAN informasi saat ini menjadi hal yang sangat penting, terutamaterhadap organisasi yang menggunakan teknologi Informasi(TI) sebagai pendukung proses bisnisnya dan KPPN Surabaya I merupakan organisasi pemerintahan yang menggunakan TI untuk mendukung proses bisnisnya. Penggunaan TI di KPPN Surabaya I bertujuan untuk meningkatkan kualitas layanan yang diberikan terhadap para *stakeholder*. Terkait dengan pentingnya keamanan informasi, maka pada tahun 2010 Kementerian Keuangan mengeluarkan Keputusan Menteri Keuangan Nomor 479/KMK.01/2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan.

Dukungan keamanan informasi bertujuan agar informasi yang dimiliki terjamin kerahasiaannya (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availability*). Salah satu bentuk dukungan keamanan informasi adalah dengan adanya tata kelola keamanan informasi agar risiko keamanan informasi dapat dikurangi atau dihindari. Keamanan informasi merupakan aspek penting dari tata kelola organisasi, kinerja TI akan terganggu jika keamanan informasi sebagai aspek penting dari keamanan informasi mengalami masalah terkait kerahasiaannya (confidentiality), keutuhannya (integrity) dan ketersediaannya (availibility). Keamanan informasi secara tidak langsung akan mempengaruhi kegiatan operasional yang dilakukan KPPN Surabaya I.

Salah satu tugas pokok KPPN Surabaya I adalah menyalurkan pembiayaan yang dibebankan pada Anggaran Pendapatan Belanja Negara (APBN). Transaksi-transaksi yang terjadi merupakan aset informasi yang dimiliki KPPN Surabaya I. Data transaksi-transaksi yang terjadi nantinya akan dijadikan laporan yang mencerminkan tingkat penyerapan APBN. Kontrol akses terhadap transaksi yang terjadi merupakan hal penting agar informasi yang ada terjamin kerahasiaannya (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availibility*). Sampai saat ini, KPPN Surabaya I belum memiliki tata kelola keamanan informasi lebih khusus lagi terhadap kontrol akses.

Permasalahan tersebut di atas mendorong penulis untuk membuat tata kelola keamanan informasi yang fokus pada kontrol akses pada KPPN Surabaya I. Tata kelola ini dibuat dengan mengacu pada kerangka kerja ISO/IEC 27001:2005.

Permasalahan yang akan diselesaikan dalam tugas akhir ini adalah :

1) Bagaimana mengidentifikasi dan menganalisis risiko keamanan informasi yang berhubungan dengan akses kontrol yang terdapat di KPPN Surabaya I?
2) Bagaimana pengimplementasian tata kelola keamanan informasi yang berfokus pada kontrol akses menurut ISO/IEC 27001:2005?

Tujuan yang diharapkan dalam tugas akhir ini adalah membuat sebuah dokumen tata kelola keamanan informasi berdasarkan ISO/IEC 27001:2005 yang berfokus pada kontrol akses pada KPPN Surabaya I.

Tugas akhir ini diharapkan dapat memberikan manfaat antara lain:

1. Membantu pengelolaan keamanan informasi pada KPPN Surabaya I sehingga akan meningkatkan kinerja KPPN Surabaya I itu sendiri.
2. Dokumen tata kelola ini nantinya dapat dijadikan pedoman dalam pengelolaan keamanan informasi pada KPPN lain.

II. TINJAUAN PUSTAKA

A. Tinjauan Pustaka

Beberapa definisi tata kelola TI menurut beberapa sumber antara lain :

- Tata kelola TI menjelaskan *decision rights* dan *accountability* framework untuk mendorong perilaku yang diinginkan dalam menggunakan TI [1].
- Tata kelola TI didefinisikan sebagai struktur hubungan dan proses untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis dapat tercapai melalui penambahan nilai sekaligus melalui penyeimbangan risiko terkait dengan pengelolaan proses TI. Tidak hanya pengelolaan proses, tetapi juga memastikan bahwa proses tersebut telah dipenuhi oleh sumber daya TI yang memberikan dukungan secara optimal terhadap pemenuhan tujuan bisnis [2].

Dapat disimpulkan bahwa tata kelola TI berfokus pada keselarasan bisnis dan TI yang mengarahkan pada pemenuhan nilai bisnis dari organisasi.

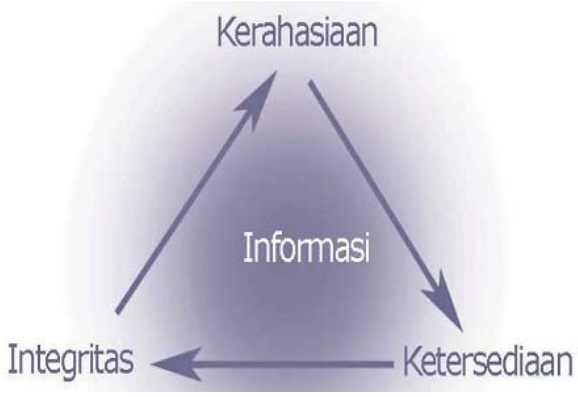
Keamanan informasi merupakan upaya untuk melindungi aset informasi yang dimiliki. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis.

Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara stimultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan [3].

Contoh keamanan informasi antara lain :

- Physical security
- Personal security
- Operation security
- Communication security
- Network security

Aspek-aspek keamanan informasi dalam suatu organisasi dapat dilihat pada gambar 1 [4]:



Gambar. 1. Aspek keamanan informasi.

- Kerahasiaan : memastikan bahwa informasi dapat di akses hanya oleh pemakai yang berwenang
- Integritas : mengamankan keakuratan dan kelengkapan informasi dan cara memproses informasi tersebut
- Ketersediaan : memastikan bahwa pemakai yang berwenang mempunyai akses terhadap informasi dan aset yang berhubungan bilamana diperlukan.

Identifikasi risiko dilakukan untuk mengidentifikasi seberapa besar dan risiko apa yang akan diterima oleh organisasi jika informasi organisasi mendapat ancaman atau gangguan keamanan yang menyebabkan gagalnya penjagaan aspek keamanan informasi [3].

Untuk mengidentifikasi risiko dilakukan langkah-langkah sebagai berikut :

- Mengidentifikasi aset yang dimiliki oleh organisasi sesuai dengan ruang lingkup SMKI serta menentukan juga pemilik asetnya
- Menghitung nilai aset berdasarkan aspek keamanan informasi
- Mengidentifikasi ancaman dan kelemahan terhadap asset
- Melakukan analisis dampak bisnis jika terjadi kegagalan penjagaan aspek keamanan informasi

Tahap selanjutnya setelah organisasi melakukan identifikasi risiko, sehingga memahami risiko yang akan dihadapi dan dampaknya terhadap organisasi adalah melakukan analisis dan evaluasi risiko. Tahap ini bertujuan untuk menganalisis dan mengevaluasi risiko yang sudah diidentifikasi pada tahap sebelumnya, untuk memahami bagaimana dampak- dampak risiko terhadap bisnis organisasi, bagaimana level risiko yang mungkin timbul dan menentukan apakah risiko yang terjad langsung diterima atau masih perlu dilakukan pengelolaan agar risiko dapat diterima dengan dampak yang bisa ditoleransi [3].

Tahap-tahap nya adalah sebagai berikut :

- Melakukan analisis dampak bisnis
- Mengestimasi level risiko
- Menentukan apakah risiko yang timbul diterima atau masih perlu pengelolaan risiko dengan menggunakan kriteria penerimaan risiko terlebih dahulu.

ISO/IEC 27001:2005 merupakan standard keamanan informasi yang diterbitkan International Organization for Standarization dan International Electrotecnical Comission pada bulan Oktober 2005 untuk menggantikan standard BS7799-2. Standard ini berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan [5].

Struktur organisasi ISO/IEC 27001 dibagi dalam dua bagian besar yaitu :

- Klausul : Mandatory process

Klausul (pasal) adalah persyaratan yang harus dipenuhi jika organisasi menerapkan SMKI dengan menggunakan standard ISO/IEC 27001

- Annex A : Security Kontrol
  Annex A adalah dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan apa (security kontrol) yang perlu diimplementasikan dalam SMKI, yang terdiri dari 11 klausul kontrol keamanan, 39 kontrol objektif dan 133 kontrol.

Standar menyatakan persyaratan utama yang harus dipenuhi menyangkut:

1. Sistem manajemen keamanan informasi (kerangka kerja, proses dan dokumentasi)
2. Tanggung jawab manajemen
3. Audit internal SMKI
4. Manajemen tinjau ulang SMKI
5. Peningkatan berkelanjutan

Disamping persyaratan utama di atas, standar ini mensyaratkan penetapan sasaran kontrol dan kontrol-kontrol keamanan informasi meliputi 11 area pengamanan sebagai berikut :

1. Kebijakan keamanan informasi
2. Organisasi keamanan informasi
3. Manajemen aset
4. Sumber daya manusia menyangkut keamanan informasi
5. Keamanan fisik dan lingkungan
6. Komunikasi dan manajemen operasi
7. Akses kontrol
8. Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
9. Pengelolaan insiden keamanan informasi
10. Manajemen kelangsungan usaha (business continuity management)
11. Kepatuhan

III. METODOLOGI

Metologi penelitian yang digunakan dalam tugas akhir ini secara garis bersar terdiri dari 4(empat) tahapan pengerjaan yaitu :

1. Pengumpulan data
2. Analisis data
3. Pembuatan dokumen tata kelola
4. Verifikasi dokumen tata kelola

Penjelasan lebih lanjut terhadap metodologi yang digunakan terdapat di bagian empat(pembahasan).

IV. PEMBAHASAN

4.1. *Pengumpulan Data*

Tahap pengumpulan data dilakukan untuk memperoleh pemahaman terhadap permasalahan dan proses bisnis yang terjadi di KPPN Surabaya I yang berkaitan dengan penegelolaan kontrol akses. Pengumpulan data dilakukan dengan menggunakan metode observasi dan wawancara terhadap pihak-pihak di KPPN Surabaya I baik Kepala Seksi, Supervisor dan pelaksana.

4.2. Analisis data

Tahapan analisis data dibagi menjadi 3 (tiga) tahapan utama yaitu identifikasi risiko, analisis risiko dan penetuan tujuan kontrol.

4.2.1. Identifikasi Risiko

Identifikasi risiko dikerjakan melalaui beberapa tahap pengerjaan seperti :

4.2.1.1. Identifikasi Aset

Identifikasi aset bertujuan untuk menentukan aset yang berhubungan dengan kontrol akses di KPPN Surabaya I. Berdasarkan hasil observasi yang dilakukan maka aset yang teridentifikasi dapat dilihat pada tabel 1.

Tabel 1.
Identifikasi jenis aset dan aset

No	Jenis Aset	Aset
1	Aset Perangkat Keras	PC, Server, Jaringan Fisik
2	Aset Perangkat Lunak	Sistem Operasi, Aplikasi KPPN
3	Data	Data user dan password

4.2.1.2. Menghitung Nilai Aset

Setelah aset sudah teridentifikasi maka langkah berikutnya adalah melakukan penilaian aset berdasarkan pendekatan tiga aspek keamanan informasi yaitu kerahasiaan(confidentiality), keutuhan (integrity) dan ketersediaan (availiability). Perhitungan tersebut dilakukan mengggunakan persamaan matematis sebagai berikut :

$$\text{Nilai Aset (NA)} = NC + NI + NV$$

Dari hasil wawancara dan observasi yang dilakukan diperoleh nilai dari masing-masing aset yang dapat dilihat pada tabel 2 .

Tabel 2.
Nilai aset yang teridentifikasi

No	Aset	Kriteria			Nilai Aset (NC+NI+NV)
		Nilai Confidentiality (NC)	Nilai Integrity (NI)	Nilai Availability (NA)	
1	PC	2	2	3	7
2	Server	3	3	3	9
3	Jaringan	2	2	3	7
3	OS	2	2	1	5
4	Aplikasi KPPN	2	2	2	6
6	Data User dan password	3	3	3	9

4.2.1.3. Identifikasi ancaman dan kelemahan aset

Setelah aset ditentukan nilainya maka langkah berikutnya adalah mengidentifikasi ancaman atau kelemahan terhadap masing-masing aset, kemudian ditentukan nilai rerata probabilitas kemunculan ancaman dan kelemahannya dengan menggunakan rentang nilai sebagai berikut :

- Low : Nilai rerata probabilitas 0,0 – 0,3
- Medium : Nilai rerata probabilitas 0,4 – 0,6
- High : Nilai rerata probabilitas 0,7 – 1,0

Nilai rerata probabilitas tiap ancaman dan kelemahan yang muncul dihitung menggunakan rata-rata kejadian yang terjadi

di KPPN Surabaya I dibagi jumlah hari kerja dalam satu bulan. Nilai probabilitas ancaman dan nilai ancaman dari masing-masing aset dapat dilihat pada tabel 3:

Tabel 3.
Nilai probabilitas ancaman dan nilai ancaman aset

Aset	Kejadian	Jenis (ancaman/kelemahan)	Probabilitas (low/med/high)	Kejadian	Nilai Probabilitas (PO)	∑ PO	Nilai Ancaman (NT)
PC	Pencurian PC	Ancaman	Low	0	0.0	0.00	0.00
Server	Pencurian Server	Ancaman	Low	0	0.0	0.00	0.00
	Akses terhadap server selain oleh supervisor	Ancaman	Low	0	0.0	0.00	0.00
Jaringan	Akses Ilegal	Ancaman	Low	0	0.0	0.00	0.00
	Pencurian perangkat	Ancaman	Low	0	0.0		
Sistem Operasi	Tidak terupdatenya OS	Kelemahan	Low	2	0.1	1.02	0.25
	Serangan virus	Ancaman	High	10	0.5		
	Kegagalan operasional	Kelemahan	Low	0	0.0		
	Penggunaan hak akses administrator pada pc pengguna	Kelemahan	High	20	0.4		
Aplikasi KPPN	Aplikasi yang tidak terupdate	Kelemahan	Low	4	0.2	0.45	0.11
	serangan virus	Ancaman	Low	0	0.0		
	kegagalan operasional	Kelemahan	Low	5	0.3		
User dan password	Tidak adanya prosedur pendaftaran user dan password	Kelemahan	Low	2	0.10	0.54	0.11
	User dan password pegawai yang pindah dan belum dihapus	Kelemahan	Low	0	0.00		
	password dengan panjang kurang dari 6 karakter	Kelemahan	* Low	8	0.16		
	Penggunaan user dan password oleh pengguna lain	Ancaman	Low	0	0.00		
	penggunaan password awal yang tidak dirubah	Kelemahan	* Low	9	0.28		

4.2.2. Analisis Risiko

Analisis risiko dilakukan melalui beberapa tahapan pengerjaan seperti :

4.2.2.1. Analisa dampak bisnis(Business Impact Analysis/BIA)

Analisa dampak bisnis dilakukan untuk mengambarkan tingkat ketahanan proses bisnis yang dijalankan KPPN Surabaya I saat aset yang dimilikinya terganggu. Nilai BIA dibuat untuk mengetahui batas toleransi dari aset yang ada terhadap ancaman dan kelemahan yang muncul. Kriteria penilaian untuk BIA dapat dilihat pada tabel 4:

Tabel 4.
Kriteria nilai BIA

Batas toleransi gangguan	Keterangan	Nilai BIA
< 1 minggu	Not critical	0
1 – 2 hari	Minor critical	1
< 1 hari	Mayor critical	2
< 12 jam	High critical	3
< 1 jam	Very high critical	4

Dengan menggunakan nilai kriteria BIA yang sudah ditentukan maka berikutnya dapat dibuat tabel dampak bisnis terhadap aset-aset yang dimiliki KPPN Surabaya I yang dapat dilihat pada tabel 5.

Tabel 5.
Nilai BIA untuk masing-masing aset

Aset	Dampak	Nilai BIA
PC	Pelayanan prima 1 jam tidak dapat tercapai	1
Server	Kegiatan pelayanan terhadap satker terhenti	4
Jaringan	Komunikasi data/informasi terhenti sehingga menggangu jalannya pelayanan terhadap satker	4
OS	Pelayanan terhadap satker terganggu sehingga dapat menghambat janji pelayanan prima 1 jam serta menghambat	3
Aplikasi KPPN	Pelayanan terhadap satker terganggu sehingga dapat menghambat janji pelayanan prima 1 jam.	3
Data User dan password	Pelayanan terhadap satker dan pekerjaan operasional terganggu sehingga janji layanan 1 jam tidak tercapai	4

4.2.2.2. Identifikasi Level Risiko

Penilaian level risiko melibatka dua cara pandang, yaitu penilaian berdasarka level probabilitas terjadinya ancaman serta level dampak dari risiko yang muncul. Untuk memudahkannya maka dibuatkan sebuah matriks level risiko dari kedua cara pandang tersebut, matriks tersebut dapat dilihat pada tabel 6 .

Tabel 6.
Matriks Level Risiko

Probabilitas Ancaman	Dampak bisnis				
	Not critical 0	Low critical 1	Medium critical 2	High critical 3	Very high critical 4
Low (0,1)	Low 0	Low 0,1	Low 0,2	Low 0,3	Low 0,4
Medium (0,5)	Low 0	Medium 0,5	Medium 1	Medium 1,5	Medium 2
High (1,0)	Low 0	Medium 1	Medium 2	High 3	High 4

4.2.2.3. Menentukan risiko diterima atau dilakukan pengelolaan risiko

Untuk menentukan sebuah risiko diterima atau perlu dilakukan pengelolaan terhadap risiko tersebut, maka perlu diketahui nilai dari risiko. Nilai risiko dihitung dengan menggunakan rumus :

$$\text{Risk Value} = NA \times BIA \times NT$$

Dari beberapa perhitngan yang sudah dilakukan sebelumnya, maka dapat ditentukan nilai dari masing-masing aset seperti terlihat pada tabel 7.

Tabel 7.
Nilai Risiko

Nomor	Aset	Nilai Aset	Nilai Ancaman	BIA	Nilai Risiko
1	PC	7	0.00	1.00	0
2	Server	9	0.00	4.00	0
3	Jaringan	7	0.00	4.00	0
4	OS	5	0.25	3.00	3.75
5	Aplikasi	6	0.11	3.00	1.98
6	User/password	9	0.11	4.00	3.96

Setelah didapatkan nilai risiko, maka langkah berikutnya adalah menentukan level risiko. Level risiko didapatkan dengan meneyesuaikan nilai risiko yang didapatkan ke dalam matriks level risiko sehingga diperoleh hasil level risiko untuk masing-masing aset dapat dilihat pada tabel 8 :

Tabel 8.
Level Risiko

No	Aset	Nilai Risiko (RV)	Level Risiko
1	PC	0	Low
2	Server	0	Low
3	Jaringan	0	Low
4	OS	3.75	High
5	Aplikasi KPPN	1.98	Medium
6	Data User dan password	3.96	High

Berdasarkan hasil perhitungan tersebut, maka aset dengan risiko yang bernilai *high* saja yang akan dilakukan pengelolaan risikonya dan aset tersebut adalah :

1. Sistem Operasi (OS)
2. Data user dan password

4.2.3. Penentuan Tujuan Kontrol

Tujuan kontrol yang digunakan didasarkan dari tujuan kontrol yang terdapat pada Annex A ISO/IEC 27001:2005 yang disesuaikan dengan ancaman dan kelemahan risiko pada klausul kontrol akses (klausul 10). Tujuan kontrol kemudian dijadikan dasar untuk membuat prosedur kontrol dalam pengelolaan risiko. Berikut adalah tujuan kontrol yang digunakan untuk masing-masing aset yang dikelola risikonya :

1. Sistem Operasi

Kategori Keamanan Utama A.11.5 : Kontrol Akses Sistem Operasi Objektif Kontrol : Untuk mencegah akses tanpa hak ke sistem operasi		
A.11.5.1	Prosedur *log-on* yang aman	Kontrol : Akses terhadap sistem operasi seharusnya dikontrol dengan prosedur *log-on* yang aman.
A.11.5.2	Identifikasi dan autentifikasi pengguna	Seluruh pengguna harus mempunyai ID yang unik untuk penggunaan pribadi dan teknik autentifikasi yang tepat harus dipilih untuk memastikan identitas pengguna
Kategori Keamanan Utama A.11.2 : Manajemen akses user Objektif Kontrol : Untuk memastikan pengguna yang mempunyai hak akses ke Sistem Informasi dan yang tidak		
A.11.2.1	Registrasi pengguna	Kontrol : Harus ada prosedur formal untuk registrasi dan penghapusan user atau pengguna untuk pemberian dan pencabutan akses ke seluruh Sistem Informasi dan layanan.
A.11.2.4	Tinjauan terhadap hak akses user	Manajemen harus melakukan tinjauan ulang hak akses user secara berkala melalui proses yang formal

2. Data user dan password

Kategori Keamanan Utama A.11.3 : Tanggung jawab pengguna (*user*) Objektif Kontrol : Untuk mencegah akses user tanpa hak atau pencurian informasi dan fasilitas pemrosesan informasi		
A.11.3.1	Penggunaan Password	Kontrol : Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan password

4.3. Pembuatan Dokumen

Pembuatan dokumen dilakukan melalui beberpa tahapan sebagai berikut :

4.3.1. Pembuatan Pedoman Manual Keamanan Informasi (MKI)

Pembuatan MKI bertujuan untuk menjelaskan kepada seluruh pihak di organisasi mengenai komitmen organisasi dalam menjaga keamanan informasi. MKI sendiri terdiri dari 7 bagian :

- Pendahuluan (MK.01)
- Ruang Lingkup(MK.02)
- Istilah dan definisi(MK.03)
- Sistem manajemen keamanan informasi(MK.04)
- Tanggungjawab manajemen(MK.05)
- Audit internal(MK.06)
- Tinjauan manajemen(MK.07)
- Peningkatan SMKI(MK.08)

4.3.2. Pembuatan Prosedur Keamanan Informasi

Prosedur Keamanan Informasi merupakan penjabaran dari Manual Keamanan Informasi. Dokumen ini terdiri atas :

- Prosedur pengendalian dokumen(PK.01)
- Prosedur pengendalian rekaman (PK.02)
- Prosedur pengendalian hak akses(PK.03)
- Prosedur log on(PK.04)
- Audit internal(PK.05)
- Prosedur tinjauan manajemen(PK.06)
- Prosedur perbaikan dan pencegahan(PK.07)

4.3.3. Pembuatan Instruksi Kerja

Instruksi Kerja merupakan dokumen teknis yang berisi petunjuk serta arahan yang dibuat secara praktis dan mudah

dipahami oleh pelaksana teknis. Berikut adalah instruksi kerja yang dibuat ;

- Registrasi pengguna(IK.01)
- Review pengguna(IK.02)

4.3.4. Pembuatan Referensi

- Struktur Organisasi (RF1)
- Uraian Tugas (RF-2)
- Kebijakan Keamanan Informasi (RF-3)
- Laporan Perkiraan Risiko (RF-4)
- Daftar Dokumentasi SMKI (RF-5)
- SoA (RF-6)

4.3.5. Pembuatan Formulir

- Daftar Dokumen Eksternal (FM-01)
- Formulir perubahan dokumen (FM-02)
- Formulir pembuatan dokumen (FM-03)
- Masterlist dokumen (FM-04)
- Daftar rekaman keamanan informasi (FM-05)
- Formulir pendaftaran / penghapusan hak akses (FM-06)
- Formulir laporan ketidaksesuaian (FM-07)

4.4. Verifikasi Dokumen

Verifikasi dokumen dilakukan dengan membandingkan persyaratan kelengkapan yang terdapat pada ISO/IEC 27001:2005 dengan dokumen yang sudah dibuat. Verifikasi dilakukan dengan melakukan pengisian tabel verifikasi yang dapat dilihat pada tabel 9.

Tabel 9.
Verifikasi Dokumen

No	Persyaratan Dokumen ISO/IEC 27001:2005	Nama Dokumen	Nomor	Ket
1	Pernyataan Kebijakan			
2	Ruang lingkup			
3	Prosedur dan kontrol pendukung SMKI			
4	Deskripsi metodologi penilaian risiko			
5	Laporan perkiraan risiko			
6	Rencana pengelolaan risiko			
7	Dokumentasi prosedur yang dibutuhkan oleh organisasi			
8	Rekaman yang dibutuhkan oleh standar ISO 27001:2005			
9	Statement of applicability			

V. KESIMPULAN

Simpulan yang diperoleh dari pengerjaan tugas akhir ini adalah sebagai berikut :

1. Masih kurangnya kesadaran tentang keamanan informasi pada KPPN Surabaya I yang terlihat dari hasil identifikasi ancaman maupun kelemahan yang dilakukan.
2. Terdapat dua aset yang perlu dilakukan pengelolaan risikonya karena memiliki nilai risiko yang tinggi, yaitu Sistem operasi dan data user/password
3. Pembuatan dokumen tata kelola ini menghasilkan dokumen manual keamanan informasi, dokumen prosedur keamanan informasi, instruksi kerja serta formulir.

UCAPAN TERIMA KASIH

Penulis M.U mengucapkan terimakasih terhadap Direktorat Jenderal Perbendaharaan dan KPPN Surabaya I yang telah banyak membantu sehingga penelitian ini dapat terlaksana.

DAFTAR PUSTAKA

[1] Weill, Peter., Ross, Jeanne W. 2004**.** *IT Governance: How top performers manage IT decision rights for superior results.* Harvard Business Press.

[2] Sarno, Riyanarto. 2009. Audit Sistem & Teknologi Informasi. Surabaya: ITS Press 2ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management System – Requirements, 15 Oktober 2005

[3] Sarno, Riyanarto., Iffano, Irsyat 2009. Sistem Manajemen Keamanan Informasi berbasis ISO 27001. Surabaya: ITS Press

[4] Triantono, H. B. (2007). Kebijakan Keamanan Dengan Standar BS 7799/ ISO 17799. Seminar Nasional Teknologi Informasi 2007 (SNATI 2007), (hal. 75-78). Yogyakarta. 4

[5] Tim Direktorat Keamanan Informasi Depkominfo. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. 5Menteri Keuangan Republik Indonesia. 2010. KMK Nomor 479/KMK.01/2010 tanggal 13 Desember 2010